

PATENT
81942.0015
Express Mail Label No. EL 713 626 455 US



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Kiyoko KATAYANAGI et al.

Serial No: Not assigned

Filed: May 21, 2001

For: ENCRYPTION METHOD, DECRYPTION METHOD,
CRYPTOGRAPHIC COMMUNICATION METHOD,
CRYPTOGRAPHIC COMMUNICATION SYSTEM, MEMORY
PRODUCT AND DATA SIGNAL EMBODIED IN CARRIER
WAVE

Art Unit: Not assigned

Examiner: Not assigned

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith are certified copies of Japanese patent application Nos. 2000-153358 filed May 24, 2000 and 2000-307822 filed October 6, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: May 21, 2001

By: 

Michael Crapenhof
Registration No. 37,115
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

JC971 U.S. PTO
09/862888
05/21/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application:

2000年 5月24日

出願番号
Application Number:

特願2000-153358

出願人
Applicant(s):

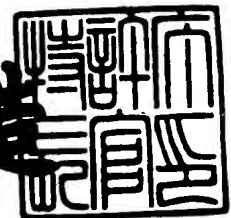
村田機械株式会社
笠原 正雄

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 3月23日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3023000

【書類名】 特許願

【整理番号】 21218

【提出日】 平成12年 5月24日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00
H04K 1/00

【発明の名称】 暗号化方法，復号方法，暗号通信システム及び記録媒体

【請求項の数】 12

【発明者】

 【住所又は居所】 滋賀県大津市仰木の里東8丁目7-12

 【氏名】 片柳 磨子

【発明者】

 【住所又は居所】 京都府京都市伏見区竹田向代町136番地 村田機械株式会社 本社工場内

 【氏名】 村上 恭通

【発明者】

 【住所又は居所】 大阪府箕面市粟生外院4丁目15番3号

 【氏名】 笠原 正雄

【特許出願人】

 【識別番号】 000006297

 【氏名又は名称】 村田機械株式会社

 【代表者】 村田 純一

【特許出願人】

 【識別番号】 597008636

 【氏名又は名称】 笠原 正雄

【代理人】

 【識別番号】 100078868

 【弁理士】

 【氏名又は名称】 河野 登夫

【電話番号】 06-6944-4141

【選任した復代理人】

【識別番号】 100114557

【弁理士】

【氏名又は名称】 河野 英仁

【電話番号】 06-6944-4141

【手数料の表示】

【予納台帳番号】 001889

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9805283

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化方法、復号方法、暗号通信システム及び記録媒体

【特許請求の範囲】

【請求項1】 平文から暗号文を得る暗号化方法において、暗号化すべき平文を K 分割してなる K 個の成分を有する第1ベクトルに R 個の任意の乱数を成分とする第2ベクトルを加えた $(K+R)$ 個の成分を有する第3ベクトルと、整数 d_i ($1 \leq i \leq K+R$) を用いて $(K+R)$ 個の各成分 D_i が $D_i = d / d_i$ (但し、 $d = d_1 d_2 \cdots d_{K+R}$ (任意の2つの整数 d_i , d_j は互いに素)) に設定された第4ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項2】 平文から暗号文を得る暗号化方法において、暗号化すべき平文を K 分割してなる K 個の成分を有する第1ベクトルに R 個の任意の乱数を成分とする第2ベクトルを加えた $(K+R)$ 個の成分を有する第3ベクトルと、整数 d_i ($1 \leq i \leq K+R$) 及び乱数 v_i を用いて $(K+R)$ 個の各成分 V_i が $V_i = (d / d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_{K+R}$ (任意の2つの整数 d_i , d_j は互いに素)) に設定された第4ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項3】 平文から暗号文を得る暗号化方法において、暗号化すべき平文を K 分割してなる K 個の成分を有する第1ベクトルに R 個の任意の乱数を成分とする第2ベクトルを加えた $(K+R)$ 個の成分を有する第3ベクトルと、複数の整数 d_i ($1 \leq i \leq K+R$) を用いて各組毎に $(K+R)$ 個の各成分 D_i が $D_i = d / d_i$ (但し、 $d = d_1 d_2 \cdots d_{K+R}$ (任意の2つの整数 d_i , d_j は互いに素)) に設定された複数の第4ベクトルとを用いて暗号文を得ることを特徴とする暗号化方法。

【請求項4】 平文から暗号文を得る暗号化方法において、暗号化すべき平文を K 分割してなる K 個の成分を有する第1ベクトルに R 個の任意の乱数を成分とする第2ベクトルを加えた $(K+R)$ 個の成分を有する第3ベクトルと、複数の整数 d_i ($1 \leq i \leq K+R$) 及び乱数 v_i を用いて各組毎に $(K+R)$ 個の各成分 V_i が $V_i = (d / d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_{K+R}$ (任意の2つの整数 d_i , d_j は互いに素)) に設定された複数の第4ベクトルとを用い

て暗号文を得ることを特徴とする暗号化方法。

【請求項5】 前記第3ベクトルの各成分と、前記第4ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分とによる積和演算により暗号文を得るようにした請求項1～4の何れかに記載の暗号化方法。

【請求項6】 平文から暗号文を得る暗号化方法において、

暗号化すべき平文をK分割してなる平文ベクトル $m = (m_1, m_2, \dots, m_K)$ に任意の乱数を成分とする疑似平文ベクトル $m' = (m_{K+1}', m_{K+2}', \dots, m_{K+R}')$ を加えた拡大平文ベクトル $m'' = (m_1'', m_2'', \dots, m_{K+R}'')$ と、整数 d_i ($1 \leq i \leq K+R$) を用いて $D_i = d / d_i$ (但し、 $d = d_1 d_2 \dots d_{K+R}$ (任意の2つの整数 d_i, d_j は互いに素)) に設定された基数ベクトル $D = (D_1, D_2, \dots, D_{K+R})$ とを用いて、前記平文を暗号文に変換することとし、

(K+R)個の乱数 v_i を生成して、式(a)により変換基数積 V_i を導くステップと、

$$V_i = D_i v_i \quad \dots (a)$$

式(b)により定義される積和平文Mに対して、 $M < P$ を満たす素数Pを生成するステップと、

$$M = m_1'' V_1 + m_2'' V_2 + \dots + m_{K+R}'' V_{K+R} \quad \dots (b)$$

$w < P$ を満たす乱数wを定め、式(c)により公開鍵ベクトル $c = (c_1, c_2, \dots, c_{K+R})$ を求めるステップと、

$$c_i \equiv w V_i \pmod{P} \quad \dots (c)$$

拡大平文ベクトル m'' と公開鍵ベクトル c との内積により、式(d)に示す暗号文Cを作成するステップと

$$C = m_1'' c_1 + m_2'' c_2 + \dots + m_{K+R}'' c_{K+R} \quad \dots (d)$$

を有することを特徴とする暗号化方法。

【請求項7】 請求項6にて得られた暗号文を復号する復号方法であって、前記暗号文Cに対して、積和平文Mを式(e)のようにして求めるステップと

$$M \equiv w^{-1} C \pmod{P} \quad \dots (e)$$

積和平文Mに対して、平文ベクトルmを式(f)のようにして復号するステップと

$$m_i \equiv M V_i^{-1} \pmod{d_i} \quad \dots (f)$$

を有することを特徴とする復号方法。

【請求項8】 平文から暗号文を得る暗号化方法において、

暗号化すべき平文をK分割してなる平文ベクトル $m = (m_1, m_2, \dots, m_K)$ に任意の乱数を成分とする疑似平文ベクトル $m' = (m_{K+1}', m_{K+2}', \dots, m_{K+R}')$ を加えた拡大平文ベクトル $m'' = (m_1'', m_2'', \dots, m_{K+R}'')$ と、素数P, Qに関して2組の整数 $d_i^{(P)}, d_i^{(Q)}$, ($1 \leq i \leq K+R$)を用いて $D_i^{(P)} = d^{(P)} / d_i^{(P)}$ (但し、 $d^{(P)} = d_1^{(P)} d_2^{(P)} \dots d_{K+R}^{(P)}$ (任意の2つの整数 $d_i^{(P)}, d_j^{(P)}$ は互いに素)), $D_i^{(Q)} = d^{(Q)} / d_i^{(Q)}$ (但し、 $d^{(Q)} = d_1^{(Q)} d_2^{(Q)} \dots d_{K+R}^{(Q)}$ (任意の2つの整数 $d_i^{(Q)}, d_j^{(Q)}$ は互いに素))に設定された2つの基数ベクトル $D^{(P)}, D^{(Q)}$ とを用いて、前記平文を暗号文に変換することとし、

2組の $(K+R)$ 個の乱数 $v_i^{(P)}, v_i^{(Q)}$ を生成して、式(g), (h)により変換基数積 $V_i^{(P)}, V_i^{(Q)}$ を導くステップと、

$$V_i^{(P)} = D_i^{(P)} v_i^{(P)} \quad \dots (g)$$

$$V_i^{(Q)} = D_i^{(Q)} v_i^{(Q)} \quad \dots (h)$$

中国人の剰余定理を用いて、P, Qによる余りが夫々 $V_i^{(P)}, V_i^{(Q)}$ となるような最小の変換基数積 $V_i^{(N)}$ ($N = PQ$)を求めるステップと、

変換基数積 $V_i^{(N)}$ と拡大平文ベクトル m'' とを用いて、式(i)により積和平文Mを定義するステップと、

$$M = m_1'' V_1^{(N)} + m_2'' V_2^{(N)} + \dots + m_{K+R}'' V_{K+R}^{(N)} \quad \dots (i)$$

$w < N$ を満たす乱数wを定め、式(j)により公開鍵ベクトル $c = (c_1, c_2, \dots, c_{K+R})$ を求めるステップと、

$$c_i \equiv w V_i \pmod{N} \quad \dots (j)$$

拡大平文ベクトル m'' と公開鍵ベクトルcとの内積により、式(k)に示す暗号文Cを作成するステップと

$$C = m_1 \cdot c_1 + m_2 \cdot c_2 + \dots + m_{K+R} \cdot c_{K+R} \dots (k)$$

を有することを特徴とする暗号化方法。

【請求項 9】 請求項 8 にて得られた暗号文を復号する復号方法であって、前記暗号文 C に対して、積和平文 M を式 (1) のようにして求めるステップと

$$M \equiv w^{-1} C \pmod{N} \dots (1)$$

P, Q における積和平文 M_P , M_Q を式 (m), (n) のようにして求めるステップと、

$$M_P \equiv M \pmod{P} \dots (m)$$

$$M_Q \equiv M \pmod{Q} \dots (n)$$

式 (o), (p) によって $(m_i^{(P)}, m_i^{(Q)})$ を求め、中国人の剰余定理を適用することにより、式 (q) から平文ベクトル m を復号するステップと

【数 1】

$$m_i^{(P)} \equiv M_P V_i^{(P)-1} \pmod{d_i^{(P)}} \dots (o)$$

$$m_i^{(Q)} \equiv M_Q V_i^{(Q)-1} \pmod{d_i^{(Q)}} \dots (p)$$

$$m_i \equiv \begin{cases} m_i^{(P)} \pmod{d_i^{(P)}} \\ m_i^{(Q)} \pmod{d_i^{(Q)}} \end{cases} \dots (q)$$

を有することを特徴とする復号方法。

【請求項 10】 複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項 1～6 または 8 の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文から元の平文を復号する復号器とを備えることを特徴とする暗号通信システム。

【請求項 11】 コンピュータに、平文から積和型の暗号文を得させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体にお

いて、暗号化すべき平文を K 分割した K 個の成分を有する平文ベクトルに R 個の任意の乱数を成分とする疑似平文ベクトルを加えて $(K+R)$ 個の成分を有する拡大平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、整数 d_i ($1 \leq i \leq K+R$) 及び乱数 v_i を用いて $(K+R)$ 個の各成分 V_i が $V_i = (d/d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_{K+R}$ (任意の2つの数 d_i, d_j は互いに素)) に設定された基数ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、前記拡大平文ベクトルの各成分と前記基数ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分との積和演算により暗号文を得ることをコンピュータに実行させるプログラムコード手段とを有することを特徴とする記録媒体。

【請求項12】 コンピュータに、平文から積和型の暗号文を得させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文を K 分割した K 個の成分を有する平文ベクトルに R 個の任意の乱数を成分とする疑似平文ベクトルを加えて $(K+R)$ 個の成分を有する拡大平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、複数組の整数 d_i ($1 \leq i \leq K+R$) 及び乱数 v_i を用いて各組毎に $(K+R)$ 個の成分 V_i が $V_i = (d/d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_{K+R}$ (任意の2つの数 d_i, d_j は互いに素)) に設定された複数の基数ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、前記拡大平文ベクトルの各成分と前記複数の基数ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分との積和演算により暗号文を得ることをコンピュータに実行させるプログラムコード手段とを有することを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、公開鍵を用いて平文を暗号文に変換する公開鍵暗号系に関し、特に、積和型暗号に関する。

【0002】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュートリソースの共有」、「マルチアクセス」、「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

【0003】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【0004】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ共通鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

【0005】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵に

よって変換された暗号文は秘密鍵でのみ復号することができる。

【0006】

公開鍵暗号系の1つの方式として、積和型暗号方式が知られている。これは、送信者である一方のエンティティ側で平文をK分割した平文ベクトル $m = (m_1, m_2, \dots, m_K)$ と公開鍵である基数ベクトル $c = (c_1, c_2, \dots, c_K)$ とを用いて、暗号文 $C = m_1 c_1 + m_2 c_2 + \dots + m_K c_K$ を作成し、受信者である他方のエンティティ側でその暗号文Cを秘密鍵を用いて平文ベクトルmに復号して元の平文を得る暗号化方式である。

【0007】

このような整数環上の演算を利用した積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。そこで、本発明者等は、中国人の剰余定理を用いることにより、高速な並列復号処理を可能とした積和型暗号における暗号化方法及び復号方法を提案している（特開2000-89669号）。この暗号化方法は、基数ベクトルcの成分 c_i ($i = 1, 2, \dots, K$) を、互いに素なK個の整数 d_i を用いて $D_i = d / d_i$ （但し、 $d = d_1 d_2 \dots d_K$ ）に設定した基数 D_i を基にモジュラ変換したもの、または、互いに素なK個の整数 d_i ，乱数 v_i を用いて $D_i = (d / d_i) v_i$ に設定した基数 D_i を基にモジュラ変換したものにすることを特徴としている。このようにして、中国人の剰余定理を用いて並列に復号するので、高速な復号を行うことができる。

【0008】

【発明が解決しようとする課題】

しかしながら、この方式では、公開鍵の数を非常に大きくしない限り低密度であるので、LLL (Lenstra-Lenstra-Lovasz) アルゴリズムを用いて公開鍵と暗号文とから直接平文を求める低密度攻撃に弱い場合があるという問題があり、安全性の面での更なる改良が望まれている。

【0009】

本発明は斯かる事情に鑑みてなされたものであり、上記従来例を改良して低密

度攻撃に強く、安全性を向上できる暗号化方法及び復号方法、この暗号化方法を用いる暗号通信システム、並びに、この暗号化方法の動作プログラムを記録した記録媒体を提供することを目的とする。

【 0 0 1 0 】

【課題を解決するための手段】

請求項 1 に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文を K 分割してなる K 個の成分を有する第 1 ベクトルに R 個の任意の乱数を成分とする第 2 ベクトルを加えた $(K + R)$ 個の成分を有する第 3 ベクトルと、整数 d_i ($1 \leq i \leq K + R$) を用いて $(K + R)$ 個の各成分 D_i が $D_i = d / d_i$ (但し、 $d = d_1 d_2 \cdots d_{K+R}$ (任意の 2 つの整数 d_i , d_j は互いに素)) に設定された第 4 ベクトルとを用いて暗号文を得ることを特徴とする。

【 0 0 1 1 】

請求項 2 に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文を K 分割してなる K 個の成分を有する第 1 ベクトルに R 個の任意の乱数を成分とする第 2 ベクトルを加えた $(K + R)$ 個の成分を有する第 3 ベクトルと、整数 d_i ($1 \leq i \leq K + R$) 及び乱数 v_i を用いて $(K + R)$ 個の各成分 V_i が $V_i = (d / d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_{K+R}$ (任意の 2 つの整数 d_i , d_j は互いに素)) に設定された第 4 ベクトルとを用いて暗号文を得ることを特徴とする。

【 0 0 1 2 】

請求項 3 に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文を K 分割してなる K 個の成分を有する第 1 ベクトルに R 個の任意の乱数を成分とする第 2 ベクトルを加えた $(K + R)$ 個の成分を有する第 3 ベクトルと、複数组の整数 d_i ($1 \leq i \leq K + R$) を用いて各組毎に $(K + R)$ 個の各成分 D_i が $D_i = d / d_i$ (但し、 $d = d_1 d_2 \cdots d_{K+R}$ (任意の 2 つの整数 d_i , d_j は互いに素)) に設定された複数の第 4 ベクトルとを用いて暗号文を得ることを特徴とする。

【 0 0 1 3 】

請求項 4 に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗

号化すべき平文を K 分割してなる K 個の成分を有する第1ベクトルに R 個の任意の乱数を成分とする第2ベクトルを加えた $(K+R)$ 個の成分を有する第3ベクトルと、複数组の整数 d_i ($1 \leq i \leq K+R$) 及び乱数 v_i を用いて各組毎に $(K+R)$ 個の各成分 V_i が $V_i = (d / d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_{K+R}$ (任意の2つの整数 d_i, d_j は互いに素)) に設定された複数の第4ベクトルとを用いて暗号文を得ることを特徴とする。

【0014】

請求項5に係る暗号化方法は、請求項1～4の何れかにおいて、前記第3ベクトルの各成分と、前記第4ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分とによる積和演算により暗号文を得るようにしたことを特徴とする。

【0015】

請求項6に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文を K 分割してなる平文ベクトル $m = (m_1, m_2, \dots, m_K)$ に任意の乱数を成分とする疑似平文ベクトル $m' = (m_{K+1}', m_{K+2}', \dots, m_{K+R}')$ を加えた拡大平文ベクトル $m'' = (m_1'', m_2'', \dots, m_{K+R}'')$ と、整数 d_i ($1 \leq i \leq K+R$) を用いて $D_i = d / d_i$ (但し、 $d = d_1 d_2 \cdots d_{K+R}$ (任意の2つの整数 d_i, d_j は互いに素)) に設定された基数ベクトル $D = (D_1, D_2, \dots, D_{K+R})$ とを用いて、前記平文を暗号文に変換することとし、

$(K+R)$ 個の乱数 v_i を生成して、式(a)により変換基数積 V_i を導くステップと、

$$V_i = D_i v_i \quad \dots (a)$$

式(b)により定義される積和平文 M に対して、 $M < P$ を満たす素数 P を生成するステップと、

$$M = m_1'' V_1 + m_2'' V_2 + \dots + m_{K+R}'' V_{K+R} \quad \dots (b)$$

$w < P$ を満たす乱数 w を定め、式(c)により公開鍵ベクトル $c = (c_1, c_2, \dots, c_{K+R})$ を求めるステップと、

$$c_i \equiv w V_i \pmod{P} \quad \dots (c)$$

拡大平文ベクトル m'' と公開鍵ベクトル c との内積により、式(d)に示す暗

号文Cを作成するステップと

$$C = m_1 " c_1 + m_2 " c_2 + \dots + m_{K+R} " c_{K+R} \dots (d)$$

を有することを特徴とする。

【0016】

請求項7に係る復号方法は、請求項6にて得られた暗号文を復号する復号方法であって、

前記暗号文Cに対して、積和平文Mを式(e)のようにして求めるステップと

$$M \equiv w^{-1} C \pmod{P} \dots (e)$$

積和平文Mに対して、平文ベクトルmを式(f)のようにして復号するステップと

$$m_i \equiv M V_i^{-1} \pmod{d_i} \dots (f)$$

を有することを特徴とする。

【0017】

請求項8に係る暗号化方法は、平文から暗号文を得る暗号化方法において、暗号化すべき平文をK分割してなる平文ベクトル $m = (m_1, m_2, \dots, m_K)$ に任意の乱数を成分とする疑似平文ベクトル $m' = (m_{K+1}', m_{K+2}', \dots, m_{K+R}')$ を加えた拡大平文ベクトル $m'' = (m_1'', m_2'', \dots, m_{K+R}'')$ と、素数P, Qに関して2組の整数 $d_i^{(P)}, d_i^{(Q)}$, $(1 \leq i \leq K+R)$ を用いて $D_i^{(P)} = d^{(P)} / d_i^{(P)}$ (但し、 $d^{(P)} = d_1^{(P)} d_2^{(P)} \dots d_{K+R}^{(P)}$) (任意の2つの整数 $d_i^{(P)}, d_j^{(P)}$ は互いに素) , $D_i^{(Q)} = d^{(Q)} / d_i^{(Q)}$ (但し、 $d^{(Q)} = d_1^{(Q)} d_2^{(Q)} \dots d_{K+R}^{(Q)}$) (任意の2つの整数 $d_i^{(Q)}, d_j^{(Q)}$ は互いに素) に設定された2つの基数ベクトル $D^{(P)}, D^{(Q)}$ とを用いて、前記平文を暗号文に変換することとし、

2組の $(K+R)$ 個の乱数 $v_i^{(P)}, v_i^{(Q)}$ を生成して、式(g), (h)により変換基数積 $V_i^{(P)}, V_i^{(Q)}$ を導くステップと、

$$V_i^{(P)} = D_i^{(P)} v_i^{(P)} \dots (g)$$

$$V_i^{(Q)} = D_i^{(Q)} v_i^{(Q)} \dots (h)$$

中国人の剰余定理を用いて、P, Qによる余りが夫々 $V_i^{(P)}, V_i^{(Q)}$ とな

るような最小の変換基数積 $V_i^{(N)}$ ($N = PQ$) を求めるステップと、

変換基数積 $V_i^{(N)}$ と拡大平文ベクトル m'' とを用いて、式 (i) により積和平文 M を定義するステップと、

$$M = m_1'' V_1^{(N)} + m_2'' V_2^{(N)} + \dots + m_{K+R}'' V_{K+R}^{(N)} \quad \dots (i)$$

$w < N$ を満たす乱数 w を定め、式 (j) により公開鍵ベクトル $c = (c_1, c_2, \dots, c_{K+R})$ を求めるステップと、

$$c_i \equiv w V_i \pmod{N} \quad \dots (j)$$

拡大平文ベクトル m'' と公開鍵ベクトル c との内積により、式 (k) に示す暗号文 C を作成するステップと

$$C = m_1'' c_1 + m_2'' c_2 + \dots + m_{K+R}'' c_{K+R} \quad \dots (k)$$

を有することを特徴とする。

【0018】

請求項9に係る復号方法は、請求項8にて得られた暗号文を復号する復号方法であって、

前記暗号文 C に対して、積和平文 M を式 (1) のようにして求めるステップと

$$M \equiv w^{-1} C \pmod{N} \quad \dots (1)$$

P, Q における積和平文 M_P, M_Q を式 (m), (n) のようにして求めるステップと、

$$M_P \equiv M \pmod{P} \quad \dots (m)$$

$$M_Q \equiv M \pmod{Q} \quad \dots (n)$$

式 (o), (p) によって $(m_i^{(P)}, m_i^{(Q)})$ を求め、中国人の剰余定理を適用することにより、式 (q) から平文ベクトル m を復号するステップと

【0019】

【数 2】

$$m_i^{(P)} \equiv M_P V_i^{(P)-1} \pmod{d_i^{(P)}} \cdots (o)$$

$$m_i^{(Q)} \equiv M_Q V_i^{(Q)-1} \pmod{d_i^{(Q)}} \cdots (p)$$

$$m_i \equiv \begin{cases} m_i^{(P)} \pmod{d_i^{(P)}} \\ m_i^{(Q)} \pmod{d_i^{(Q)}} \end{cases} \cdots (q)$$

【0020】

を有することを特徴とする。

【0021】

請求項10に係る暗号通信システムは、複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項1～6または8の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文から元の平文を復号する復号器とを備えることを特徴とする。

【0022】

請求項11に係る記録媒体は、コンピュータに、平文から積和型の暗号文を得させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文をK分割したK個の成分を有する平文ベクトルにR個の任意の乱数を成分とする疑似平文ベクトルを加えて(K+R)個の成分を有する拡大平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、整数 d_i ($1 \leq i \leq K+R$) 及び乱数 v_i を用いて(K+R)個の各成分 V_i が $V_i = (d/d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_{K+R}$ (任意の2つの数 d_i, d_j は互いに素)) に設定された基数ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、前記拡大平文ベクトルの各成分と前記基数ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分との積和演算により暗号文を得ることをコンピュータに実行させるプログラムコード手段

とを有することを特徴とする。

【0023】

請求項12に係る記録媒体は、コンピュータに、平文から積和型の暗号文を得させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、暗号化すべき平文をK分割したK個の成分を有する平文ベクトルにR個の任意の乱数を成分とする疑似平文ベクトルを加えて $(K+R)$ 個の成分を有する拡大平文ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、複数组の整数 d_i ($1 \leq i \leq K+R$) 及び乱数 v_i を用いて各組毎に $(K+R)$ 個の成分 V_i が $V_i = (d/d_i) \cdot v_i$ (但し、 $d = d_1 d_2 \cdots d_{K+R}$ (任意の2つの数 d_i, d_j は互いに素)) に設定された複数の基数ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、前記拡大平文ベクトルの各成分と前記複数の基数ベクトルを基にモジュラ変換した公開鍵ベクトルの各成分との積和演算により暗号文を得ることをコンピュータに実行させるプログラムコード手段とを有することを特徴とする。

【0024】

本発明では、平文に冗長性を持たせる、言い換えると平文を退化させて暗号文を作成する。即ち、暗号化すべき平文を分割してなる第1ベクトル(平文ベクトル)及び特に暗号化を必要としない乱数成分からなる第2ベクトル(疑似平文ベクトル)を合わせた第3ベクトル(拡大平文ベクトル)と、各成分を $D_i = d/d_i$ または $V_i = (d/d_i) \cdot v_i$ に設した第4ベクトル(基数ベクトル)とを用いて暗号文を作成する。具体的には、第3ベクトル(拡大平文ベクトル)の各成分と、第4ベクトル(基数ベクトル)を基に、モジュラ変換した公開鍵ベクトルの各成分との積和演算によって暗号文を構成する。よって、暗号文の密度が高くなり、1つの暗号文に対して非常に多くの復号方法が存在するので、LLLアルゴリズムに基づく低密度攻撃は非常に困難となる。この結果、安全性が向上する。

【0025】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図 1 は、本発明による暗号化方法をエンティティ a, b 間の情報通信に利用した状態を示す模式図である。図 1 の例では、一方のエンティティ a が、暗号化器 1 にて平文 x を暗号文 C に暗号化し、通信路 3 を介してその暗号文 C を他方のエンティティ b へ送信し、エンティティ b が、復号器 2 にてその暗号文 C を元の平文 x に復号する場合を示している。

【0026】

(第 1 実施の形態)

秘密鍵と公開鍵とを以下のように準備する。

- ・秘密鍵： $\{d_i\}$, $\{d_i'\}$, $\{v_i\}$, P , w
- ・公開鍵： $\{c_i\}$

【0027】

$e > e'$ として、正規基数 d_i 及び退化基数 d_i' は、夫々下記 (1), (2) を満たす基数と定義する。

【0028】

【数 3】

$$d_i = 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \cdots (1)$$

$$d_i' = 2^{e'} + \delta_i' \quad (1 \ll \delta_i' \ll 2^{e'}) \cdots (2)$$

【0029】

($K+R$) 個の互いに素な数からなる基数を定める。但し、そのうちの $i \in I$ に対応する K 個を正規基数、 $i \in I'$ に対応する R 個を退化基数とする。ここで、 I , I' は何れもインデックス集合であり、 $I = \{1, 2, \dots, K\}$, $I' = \{K+1, K+2, \dots, K+R\}$ とし、 $I'' = I \cup I'$ とする。なお、本明細書では、特に断らない限り、 $i \in I''$ である。次に、基数積 D_i を下記 (3) に従って求める。

【0030】

【数 4】

$$D_i = \begin{cases} \frac{d_1 \dots d_K d_{K+1}' \dots d_{K+R}'}{d_i} & (i \in I) \\ \frac{d_1 \dots d_K d_{K+1}' \dots d_{K+R}'}{d_i'} & (i \in I') \end{cases} \dots (3)$$

【0031】

また、 $(K+R)$ 個の乱数 $\{v_i\}$ を生成し、変換基数積 V_i を下記 (4) により導く。

$$V_i = D_i v_i \quad \dots (4)$$

【0032】

エンティティ a 側で、エンティティ b へ暗号化して送信すべき平文 x を K 分割して、各成分が e (ビット) である平文ベクトル $m = (m_1, m_2, \dots, m_K)$ を得る。また、エンティティ b へ特に送信する必要がない各成分が e (ビット) の乱数からなる疑似平文ベクトル $m' = (m_{K+1}, m_{K+2}, \dots, m_{K+R})$ を得る。例えば、エンティティ b へ特に送信する必要がない平文 (冗長文) を R 分割して、この疑似平文ベクトル m' を得ることができる。これらの平文ベクトル m と疑似平文ベクトル m' とを結合して、 $(K+R)$ 個の成分を有する拡大平文ベクトル $m'' = (m_1'', m_2'', \dots, m_{K+R}'')$ を得る。ここで、この拡大平文ベクトル m'' の各成分は、下記 (5) のように定義される。

【0033】

【数 5】

$$m_i'' = \begin{cases} m_i & (i \in I) \\ m_i' & (i \in I') \end{cases} \dots (5)$$

【0034】

積和平文 M を、拡大平文ベクトル m'' と変換基数積 V_i とを用いて、下記 (6)

) のように定義する。

$$M = m_1 \text{ " } V_1 + m_2 \text{ " } V_2 + \cdots + m_{K+R} \text{ " } V_{K+R} \quad \cdots (6)$$

【0035】

任意の拡大平文ベクトル $m \text{ "}$ に対して、 $M < P$ を満たす素数 P を生成して法とする。素数 P より小さい乱数 w を定め、下記 (7) に従って、下記 (8) に示すような公開鍵ベクトル c を導いて公開する。

$$c_i \equiv w V_i \pmod{P} \quad \cdots (7)$$

$$\text{ベクトル } c = (c_1, c_2, \cdots, c_{K+R}) \quad \cdots (8)$$

【0036】

エンティティ a 側で、拡大平文ベクトル $m \text{ "}$ と公開鍵ベクトル c との内積を下記 (9) のように求めて、暗号文 C を得る。作成された暗号文 C は通信路 3 を介してエンティティ a からエンティティ b へ送信される。

$$C = m_1 \text{ " } c_1 + m_2 \text{ " } c_2 + \cdots + m_{K+R} \text{ " } c_{K+R} \quad \cdots (9)$$

【0037】

エンティティ b 側では、以下のようにして復号処理が行われる。

暗号文 C から積和平文 M は、下記 (10) のようにして求めることができる。

$$M \equiv w^{-1} C \pmod{P} \quad \cdots (10)$$

【0038】

拡大平文ベクトル $m \text{ "}$ のうち、正規基数に対応するインデックス、即ち、 $i \in I$ に関しては、下記 (11) が成立して、平文ベクトル m を復号することができる。

$$m_i \equiv M V_i^{-1} \pmod{d_i} \quad \cdots (11)$$

【0039】

なお、退化基数に対応するインデックス、即ち、 $i \in I'$ に関しては、復号する必要がない。また、上記 (11) と同様に下記 (12) に従って復号しようとしても、退化の影響によりビット数に関して下記 (13) の関係があるので、疑似平文ベクトル m' を正しく復号することはできない。

$$m_i \text{ " ' } \equiv M V_i^{-1} \pmod{d_i'} \quad \cdots (12)$$

$$m_i' > d_i' > m_i \text{ " ' } \quad \cdots (13)$$

【0040】

なお、上記例では、基数積 D_i に乱数 $\{v_i\}$ を付加するようにしたが、このような乱数を付加せず、上記(3)で示される基数積 D_i をそのまま用いても良い。

【0041】

(第2実施の形態)

秘密鍵と公開鍵とを以下のように準備する。

- ・秘密鍵： $\{d_i^{(P)}\}$ ， $\{d_i^{(Q)}\}$ ， $\{d_i^{(P)'}\}$ ， $\{d_i^{(Q)'}\}$ ，
 $\{v_i^{(P)}\}$ ， $\{v_i^{(Q)}\}$ ， P ， Q ， N ， w
- ・公開鍵： $\{c_i\}$

なお、上記 N は公開であっても良い。

【0042】

P ， Q を後述の条件を満たす素数とする。 $e > e'$ とし、正規基数 $d_i^{(P)}$ ， $d_i^{(Q)}$ 及び退化基数 $d_i^{(P)'}$ ， $d_i^{(Q)'}$ は、夫々下記(14)，(15)を満たす基数と定義する。

【0043】

【数6】

$$d_i^{(P)} d_i^{(Q)} = 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \cdots (14)$$

$$d_i^{(P)'} d_i^{(Q)'} = 2^{e'} + \delta_i' \quad (1 \ll \delta_i' \ll 2^{e'}) \cdots (15)$$

【0044】

法 P 及び法 Q について、夫々第1実施の形態と同様に、2組の基数 $\{d_i^{(P)}\}$ ， $\{d_i^{(P)'}\}$ 及び $\{d_i^{(Q)}\}$ ， $\{d_i^{(Q)'}\}$ を生成する。但し、任意の $i \in I''$ について、下記(16)，(17)を満たすものとする。

$$\gcd(d_i^{(P)}, d_i^{(Q)}) = 1 \quad \cdots (16)$$

$$\gcd(d_i^{(P)'}, d_i^{(Q)'}) = 1 \quad \cdots (17)$$

【0045】

次に、法 P 及び法 Q について、第1実施の形態と同様に、2組の乱数 $\{v_i^{(P)}$

$\}$ 及び $\{v_i^{(Q)}\}$ を生成し、上記 (3), (4) と同様の計算により、 $\{V_i^{(P)}\}$ 及び $\{V_i^{(Q)}\}$ を導く。

【0046】

第1実施の形態と全く同様に構成された拡大平文ベクトル m'' に対する法 P 及び法 Q における積和平文 M_P 及び積和平文 M_Q を夫々、下記 (18), (19) と定義する。

$$M_P = m_1 \text{ " } V_1^{(P)} + m_2 \text{ " } V_2^{(P)} + \dots + m_{K+R} \text{ " } V_{K+R}^{(P)} \quad \dots (18)$$

$$M_Q = m_1 \text{ " } V_1^{(Q)} + m_2 \text{ " } V_2^{(Q)} + \dots + m_{K+R} \text{ " } V_{K+R}^{(Q)} \quad \dots (19)$$

【0047】

更に、素数 P 及び素数 Q を、任意の拡大平文ベクトル m'' に対して $M_P < P$ かつ $M_Q < Q$ の条件を満たすように生成し、それらの積を N とする。中国人の剰余定理を用いて、 P 及び Q による余りが夫々 $V_1^{(P)}$ 及び $V_1^{(Q)}$ となるような最小の $V_1^{(N)}$ ($< N$) を導いて変換基数積と定義する。

【0048】

積和平文 M を、拡大平文ベクトル m'' と変換基数積 $V_1^{(N)}$ とを用いて、下記 (20) のように定義する。ここで、 $M < N$ を満たす必要はない。

$$M = m_1 \text{ " } V_1^{(N)} + m_2 \text{ " } V_2^{(N)} + \dots + m_{K+R} \text{ " } V_{K+R}^{(N)} \quad \dots (20)$$

【0049】

N より小さい乱数 w を定め、下記 (21) に従って、下記 (22) に示すような公開鍵ベクトル c を導いて公開する。

$$c_i \equiv w V_i \pmod{N} \quad \dots (21)$$

$$\text{ベクトル } c = (c_1, c_2, \dots, c_{K+R}) \quad \dots (22)$$

【0050】

エンティティ a 側で、拡大平文ベクトル m'' と公開鍵ベクトル c との内積を下記 (23) のように求めて、暗号文 C を得る。作成された暗号文 C は通信路 3 を介してエンティティ a からエンティティ b へ送信される。なお、 N を公開する場合

には、下記 (23) の C を N で割った剰余を暗号文とすれば良い。

$$C = m_1 \text{ " } c_1 + m_2 \text{ " } c_2 + \dots + m_{K+R} \text{ " } c_{K+R} \quad \dots (23)$$

【0051】

エンティティ b 側では、以下のようにして復号処理が行われる。

積和平文 M は、下記 (24) を満たす。従って、法 P 及び法 Q における積和平文 M_P 及び M_Q は、下記 (25), (26) のようにして求めることができる。

$$M \equiv w^{-1} C \pmod{N} \quad \dots (24)$$

$$M_P \equiv M \pmod{P} \quad \dots (25)$$

$$M_Q \equiv M \pmod{Q} \quad \dots (26)$$

【0052】

拡大平文ベクトル m のうち、正規基数に対応するインデックス、即ち、 $i \in I$ に関しては、 $2^e < d_i^{(P)} d_i^{(Q)}$ であるため、下記 (27), (28) によって $(m_i^{(P)}, m_i^{(Q)})$ を求め、中国人の剰余定理を適用することにより、下記 (29) が成立して、平文ベクトル m を復号することができる。

【0053】

【数7】

$$m_i^{(P)} \equiv M_P V_i^{(P)-1} \pmod{d_i^{(P)}} \quad \dots (27)$$

$$m_i^{(Q)} \equiv M_Q V_i^{(Q)-1} \pmod{d_i^{(Q)}} \quad \dots (28)$$

$$m_i \equiv \begin{cases} m_i^{(P)} \pmod{d_i^{(P)}} \\ m_i^{(Q)} \pmod{d_i^{(Q)}} \end{cases} \quad \dots (29)$$

【0054】

なお、退化基数に対応するインデックス、即ち、 $i \in I'$ に関しては、第1実施の形態と同様、復号する必要がなく、疑似平文ベクトル m' を正しく復号することができない。

【0055】

なお、上記例では、2組の基数 $\{d_i^{(P)}\}$, $\{d_i^{(Q)}\}$ に乱数 $\{v_i^{(P)}\}$

$\}, \{v_i^{(Q)}\}$ を付加するようにしたが、このような乱数を付加しない基数積を使用しても良い。

【0056】

次に、上述したような本発明の方式にあって、LLLアルゴリズムに基づく低密度攻撃に強い耐性を持てるように、1を超える高い密度を実現できていることを説明する。退化していない一般的な積和型暗号について、暗号文密度 σ ，方式密度 ρ ，レート η を下記(30)，(31)，(32)のように定義する。なお、 C は暗号文のビット数， C_{\max} は取り得る最大の暗号文のビット数， K は平文の分割数， e は分割平文のビット数である。

【0057】

【数8】

$$\sigma = \frac{\sum_{i=1}^K \log_2 m_i}{\log_2 C} \quad \dots (30)$$

$$\rho = \frac{K e}{\log_2 C_{\max}} \quad \dots (31)$$

$$\eta = \frac{K e}{|C_{\max}|} \quad \dots (32)$$

【0058】

また、本発明のように退化している積和型暗号について、暗号文密度 σ' ，方式密度 ρ' を下記(33)，(34)のように定義する。なお、レートは上記(32)と同じである。

【0059】

【数 9】

$$\sigma' = \frac{\sum_{i=1}^{K+R} \log_2 m_i''}{\log_2 C} \dots (33)$$

$$\rho' = \frac{(K+R)e}{\log_2 C_{\max}} \dots (34)$$

【0060】

第1実施の形態における密度について考察する。乱数 v_i を s ビットとする。密度をできる限り大きくするために、取り得る最大の積和平文を M_{\max} とした場合、法 P のビットサイズを $|P| = |M_{\max}|$ と設定すべきである。この場合、第1実施の形態における方式密度 ρ_1 、レート η_1 は、夫々、下記 (35)、(36) の条件を満たす。

【0061】

【数10】

$$\begin{aligned} \rho_1 &= \frac{(K+R)e}{e + \log_2 P + \log_2 (K+R)} \\ &> \frac{(K+R)e}{(K+2)e + (R-1)e' + s + 2\log_2 (K+R) + 1} \\ &\dots (35) \end{aligned}$$

$$\begin{aligned} \eta_1 &= \frac{Ke}{e + \log_2 P + \log_2 (K+R)} \\ &> \frac{Ke}{(K+2)e + (R-1)e' + s + 2\log_2 (K+R) + 1} \\ &\dots (36) \end{aligned}$$

【0062】

公開鍵より秘密鍵を求める攻撃（片柳磨子，村上恭通，笠原正雄：“積和型暗号に関する二，三の考察”，1999年暗号と情報セキュリティシンポジウム資料，B43 Jan.2000 に開示）を回避するためには、乱数 v_i のビットサイズを法 P のビットサイズの $1/4$ 以上にする必要がある。この条件を満たすように、乱数 v_i のビットサイズを $s = (1/4) \log_2 P + 1$ と考えて計算した場合、方式密度 ρ_1 ，レート η_1 は、夫々、下記 (37)，(38) の条件を満たす。

【0063】

【数11】

$$\rho_1 > \frac{3(K+R)e}{(4K+7)e + 4(R-1)e' + 7 \log_2(K+R) + 7} \dots (37)$$

$$\eta_1 > \frac{3Ke}{(4K+7)e + 4(R-1)e' + 7 \log_2(K+R) + 7} \dots (38)$$

【0064】

この条件において、乱数 v_i が非常に大きいので、 e' を $e' < e/2$ とする、または、 $K < R$ とすることにより、 $\rho_1 > 1$ を満たすパラメータが存在する。

【0065】

第2実施の形態における密度について考察する。乱数 $v_i^{(P)}$ と $v_i^{(Q)}$ との積、即ち、 $v_i^{(P)} v_i^{(Q)}$ を s ビットとする。法 N が非公開である場合、密度をできる限り大きくするために、取り得る最大の積和平文を M_{Pmax} ， M_{Qmax} としたとき、 $|P| = |M_{Pmax}|$ ， $|Q| = |M_{Qmax}|$ と設定すべきである。この場合、第2実施の形態における方式密度 ρ_2 ，レート η_2 は、夫々、下記 (39)，(40) の条件を満たす。

【0066】

【数 12】

$$\begin{aligned}\rho_2 &= \frac{(K+R)e}{e + \log_2 N + \log_2 (K+R)} \\ &> \frac{(K+R)e}{(K+3)e + (R-1)e' + s + 3\log_2 (K+R) + 1} \\ &\dots (39)\end{aligned}$$

$$\begin{aligned}\eta_2 &= \frac{Ke}{e + \log_2 N + \log_2 (K+R)} \\ &> \frac{Ke}{(K+3)e + (R-1)e' + s + 3\log_2 (K+R) + 1} \\ &\dots (40)\end{aligned}$$

【0067】

第2実施の形態では、多重化しているので、乱数をあまり大きくする必要はない。よって、 $e' = e/2$ ， $K=R$ という条件であっても、容易に方式密度 $\rho_2 > 1$ ，レート $\eta_2 > 1/2$ を達成することができる。例えば、上記の条件において、分割数を $K=8$ とし、基数 $d_i^{(P)}$ ， $d_i^{(Q)}$ 及び乱数 $v_i^{(P)}$ ， $v_i^{(Q)}$ を何れも32ビットとした場合、 $\rho_2 = 1.0174$ ， $\eta_2 = 0.5087$ となり、このような小さなパラメータでも、上記の条件（ $\rho_2 > 1$ ， $\eta_2 > 1/2$ ）を実現できている。但し、小さなパラメータでは安全性に問題があるので、例えば $K=100$ ， $e=64$ ， $e'=32$ 程度が現実的である。

【0068】

また、法 N を公開とし、 C を N で割った剰余を暗号文とした場合の第2実施の形態における方式密度 ρ_2 ，レート η_2 は、夫々、下記(41)，(42)の条件を満たす。

【0069】

【数 13】

$$\begin{aligned}\rho_2 &= \frac{(K+R)e}{\log_2 N} \\ &> \frac{(K+R)e}{(K+2)e + (R-1)e' + s + 2\log_2(K+R) + 1} \\ &\dots (41)\end{aligned}$$

$$\begin{aligned}\eta_2 &= \frac{Ke}{\log_2 N} \\ &> \frac{Ke}{(K+2)e + (R-1)e' + s + 2\log_2(K+R) + 1} \\ &\dots (42)\end{aligned}$$

【0070】

以上のように、法Nを公開とした場合には、法Nが非公開である場合に比べて、方式密度 ρ_2 ，レート η_2 の何れもが向上している。

【0071】

ところで、疑似平文ベクトル m' における乱数成分は、平文ベクトル m とは全く独立して設定できる。よって、作成した暗号文Cの方式密度が高くなるように疑似平文ベクトル m' の乱数成分を設定するようにすれば良い。また、疑似平文ベクトル m' としてある乱数系列を設定して暗号文Cを作成した後、その暗号文Cの方式密度を計算し、その計算値が1を超えない場合には、疑似平文ベクトル m' に設定する乱数系列を別なものにして暗号文Cを作成しなおすようにし、方式密度が1を超えた場合の暗号文Cを受信先のエンティティへ送信する手法が有効である。

【0072】

図2は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、第1または第2実施の形態における上述した手順に従って拡大

平文ベクトル m'' と公開鍵ベクトル c との内積計算により暗号文 C を作成する処理を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ10は、送信側のエンティティに設けられている。

【0073】

図2において、コンピュータ10とオンライン接続する記録媒体11は、コンピュータ10の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体11には前述の如きプログラム11a が記録されている。記録媒体11から読み出されたプログラム11a がコンピュータ10を制御することにより、コンピュータ10が暗号文 C を作成する。

【0074】

コンピュータ10の内部に設けられた記録媒体12は、内蔵設置される例えばハードディスクドライブまたはROMなどを用いてなり、記録媒体12には前述の如きプログラム12a が記録されている。記録媒体12から読み出されたプログラム12a がコンピュータ10を制御することにより、コンピュータ10が暗号文 C を作成する。

【0075】

コンピュータ10に設けられたディスクドライブ10a に装填して使用される記録媒体13は、運搬可能な例えば光磁気ディスク、CD-ROMまたはフレキシブルディスクなどを用いてなり、記録媒体13には前述の如きプログラム13a が記録されている。記録媒体13から読み出されたプログラム13a がコンピュータ10を制御することにより、コンピュータ10が暗号文 C を作成する。

【0076】

【発明の効果】

以上のように、本発明では、暗号化すべき平文を分割してなる第1ベクトル（平文ベクトル）に暗号化を必要としない乱数成分からなる第2ベクトル（疑似平文ベクトル）を加えた第3ベクトル（拡大平文ベクトル）と、各成分を $D_i = d / d_i$ または $V_i = (d / d_i) \cdot v_i$ に設した第4ベクトル（基数ベクトル）とを用い、積和演算方式にて暗号文を構成するようにしたので、暗号文の密度を大きくでき、LLLアルゴリズムに基づく低密度攻撃に対して強くなって安全性

を向上できる。この結果、積和型暗号の実用化の道を開くことに、本発明は大いに寄与できる。

【図面の簡単な説明】

【図 1】

2 人のエンティティ間における情報の通信状態を示す模式図である。

【図 2】

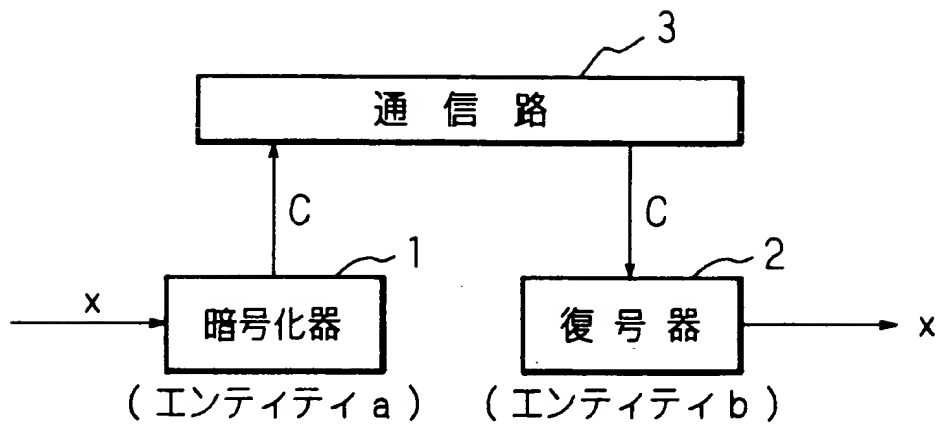
記録媒体の実施の形態の構成を示す図である。

【符号の説明】

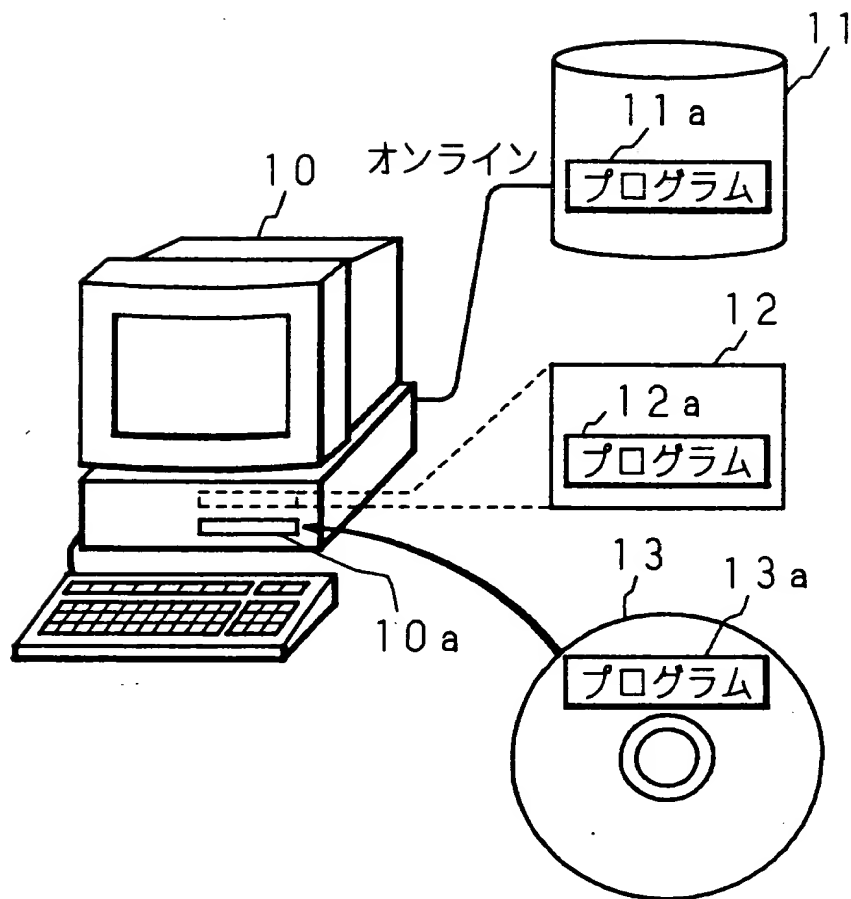
- 1 暗号化器
- 2 復号器
- 3 通信路
- a, b エンティティ

【書類名】 図面

【図 1】



【図 2】



【書類名】 要約書

【要約】

【課題】 L L L アルゴリズムに基づく低密度攻撃に強く、安全性を向上できる暗号化方法を提供する。

【解決手段】 暗号化すべき平文を K 分割した平文ベクトル $m = (m_1, m_2, \dots, m_K)$ に任意の乱数成分からなる疑似平文ベクトル $m' = (m_{K+1}', m_{K+2}', \dots, m_{K+R}')$ を加えた拡大平文ベクトル $m'' = (m_1'', m_2'', \dots, m_{K+R}'')$ と、整数 d_i ($1 \leq i \leq K+R$) 及び乱数 v_i を用いて $D_i = d / d_i \cdot v_i$ (但し、 $d = d_1 d_2 \dots d_{K+R}$ (任意の 2 つの整数 d_i, d_j は互いに素)) に設定された基数ベクトル $D = (D_1, D_2, \dots, D_{K+R})$ とを用いて、積和型の暗号文を得る。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 0 - 1 5 3 3 5 8
受付番号	5 0 0 0 0 6 4 0 7 4 3
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 2 年 5 月 2 5 日

< 認定情報・付加情報 >

【特許出願人】

【識別番号】	000006297
【住所又は居所】	京都府京都市南区吉祥院南落合町 3 番地
【氏名又は名称】	村田機械株式会社

【特許出願人】

【識別番号】	597008636
【住所又は居所】	大阪府箕面市粟生外院 4 丁目 1 5 番 3 号
【氏名又は名称】	笠原 正雄

【代理人】

申請人

【識別番号】	100078868
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目 4 番 3 号 河野 特許事務所
【氏名又は名称】	河野 登夫

【選任した復代理人】

【識別番号】	100114557
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目 4 番 3 号 河野 特許事務所
【氏名又は名称】	河野 英仁

出 願 人 履 歷 情 報

識別番号 [000006297]

1. 変更年月日 1990年 8月 7日

[変更理由] 新規登録

住 所 京都府京都市南区吉祥院南落合町3番地
氏 名 村田機械株式会社

出 願 人 履 歴 情 報

識別番号 [597008636]

1. 変更年月日	1997年 1月21日
[変更理由]	新規登録
住 所	大阪府箕面市栗生外院4丁目15番3号
氏 名	笠原 正雄